UNAM

RED·TIC
Red de Responsables TIC
U N A M

RECOMENDACIONES DE COMPARTICIÓN DE INFORMACIÓN

Noviembre de 2021, 1ª versión

Índice

Recomendaciones de compartición de información

Introducción

La información es un elemento fundamental y estratégico para las Universidades, tanto en la realización de sus actividades sustantivas como en la difusión del conocimiento, por lo que ha cobrado relevancia el intercambio y la compartición de la misma de manera efectiva y segura para cumplir con los objetivos institucionales bajo el marco normativo aplicable. Esto ha traído como consecuencia que se rompan paradigmas de islas de información y ha generado gradualmente mayor certidumbre al ser transmitida o compartida entre áreas universitarias, además de lograr mayores elementos oportunos y confiables para la toma de decisiones, así como agilizar la prestación de servicios y trámites universitarios. Para prestar estos servicios se hace uso por lo general de sistemas que permiten automatizar los procesos del quehacer diario universitario.

Propósito

Este documento es una guía que tiene como propósito orientar a los responsables de las TIC en las entidades y dependencias universitarias o aquel personal que interviene en el proceso de la compartición, transformación, uso y explotación de la información o al personal a cargo de sistemas de información; con la finalidad de aprovechar la experiencia propia o de otros, orientándolos en su aplicación a través de mecanismos para compartir e intercambiar información. Tiene la finalidad de documentar los mecanismos que permiten llevar a cabo la compartición de información, abarcando diferentes tipos de interacciones entre departamentos, entidades, dependencias y externos, facilitando el aprovechamiento de la información para el cumplimiento de las metas institucionales bajo el marco normativo aplicable.

Las recomendaciones presentadas en este documento son de consulta y uso general para todas las entidades y dependencias de la UNAM, y se busca ir enriqueciendo y liberando nuevas versiones con la retroalimentación de diferentes especialistas universitarios.

Marco legal o normativo

En México, el derecho a la información se encuentra garantizado en la Constitución Política de los Estados Unidos Mexicanos, el marco que regula la compartición de información está formado por leyes y códigos federales, lineamientos generales, así como normatividad, lineamientos y recomendaciones universitarias, los cuales se presentan en la siguiente imagen.

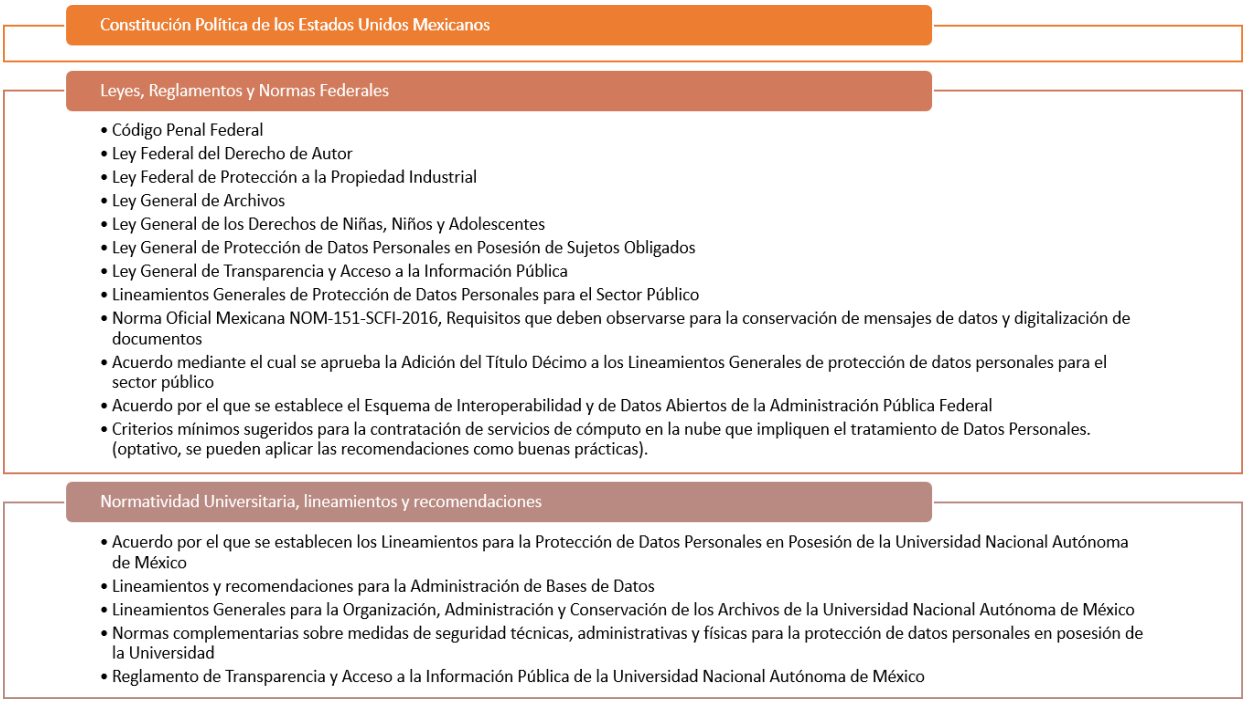


Figura 1. Marco regulatorio

Consideraciones para la compartición de información

Dentro del ciclo de vida de la información, se encuentra la etapa de uso y compartición, donde la información puede utilizarse y compartirse dentro de una misma área, entre entidades y dependencias universitarias, o con externos, entre otros; para lo cual primero debe estar clasificada con la intención de dar a conocer el tratamiento y protección que se le tiene que dar.

Clasificación de la información

Se aconseja establecer y mantener un esquema de clasificación de la información dentro de la entidad o dependencia universitaria que la posee y maneja, que defina qué tan crítica y sensible es, así como revisar qué información es pública, acorde a la legislación federal y de la UNAM aplicable.

Así, por ejemplo, la información en posesión de la UNAM es pública, salvo que se trate de datos personales, o se encuentre clasificada como reservada o confidencial de acuerdo con los supuestos previstos en los artículos 113 de la Ley General de Transparencia y Acceso a la Información Pública y 110 de la Ley Federal de Transparencia y Acceso a la Información Pública. Se recomienda contar con políticas que orienten al personal universitario a resguardar correctamente la información confidencial, asegurando que no se divulgue y tenga el tratamiento correcto de acuerdo con su clasificación, verificando los puntos aplicables de las *Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad*.

Además, se sugiere establecer acuerdos entre entidades, dependencias o con terceros, para el intercambio seguro de la información confidencial o sensible que consideren:

- Responsabilidades de gestión para controlar y notificar la transmisión, el envío y recepción.
- Niveles de control de acceso que se tendrán acorde a la clasificación de la información.
- Procedimientos para asegurar la trazabilidad y no repudio.
- Normas técnicas mínimas para el empaquetado y transmisión, uso de controles criptográficos y canales seguros de comunicación.
- Mecanismos e interfaces para compartir o intercambiar información.
- Suscribir acuerdos de confidencialidad y no divulgación, en los cuales se especifique la información a proteger y los usos permitidos de la misma, así como también las responsabilidades, los procesos para notificar y reportar la divulgación no autorizada o brechas de seguridad ocurridas, el derecho de auditar y de supervisar actividades que involucran información confidencial.
- Acuerdos sobre la custodia de la información a compartir e intercambiar.
- Responsabilidades y compromisos en caso de incidentes de seguridad, tales como pérdida de datos.

Mecanismos de compartición de información

La información se puede compartir a través de mecanismos acordados entre las entidades y dependencias universitarias involucradas para lo cual se aconseja considerar las siguientes prácticas generales:

- Identificar de acuerdo con los procedimientos y medios establecidos, la entidad o dependencia universitaria que emite la información a compartir, así como la que recibe los datos.
- Garantizar el nivel de confidencialidad requerido.
- Contar con una traza de la operación realizada que pueda ser auditada en caso necesario.
- Definir una política de seguridad para el acceso, transmisión y recepción.
- Incorporar controles de seguridad en aspectos como la seguridad física, el uso de prácticas de desarrollo seguro, las revisiones periódicas de seguridad, por mencionar algunas.

A continuación, se describen como referencia algunos mecanismos de compartición de información ampliamente utilizados:

Servicios web

Características

Los servicios web (en inglés web services) permiten la comunicación entre sistemas por medio de protocolos web estándar, usando mensajes escritos en XML. Las implementaciones más comunes son: SOAP (Simple Object Access Protocol) y RESTful.

Recomendaciones

Para facilitar la compartición de información se recomienda establecer los metadatos que conformarán el XML generado por el servicio web, determinar los parámetros de entrada y salida de cada servicio web que defina su propósito, así como el uso de etiquetas descriptivas.

Así mismo, una buena práctica es documentar el servicio web realizando una descripción del servicio, al menos un documento WSDL (Web Service Description Language) o alguno que

describa más ampliamente los metadatos ayudará a mejorar el entendimiento entre la entidad o dependencia que lo publica y aquellas que lo utilizan.

Por ejemplo, actualmente la Dirección General de Administración Escolar permite la consulta de los datos de actividades académicas de los alumnos y su vigencia mediante la solicitud formal y justificación por oficio entre los titulares de las dependencias universitarias. La documentación técnica, controles de acceso e información adicional se proporcionan a la entidad universitaria solicitante después de que la solicitud de acceso a los servicios web es revisada y aprobada.

Archivos de texto plano

Características

Los archivos de texto plano con caracteres para separar los valores contenidos en el archivo o con ancho fijo pueden ser un medio para compartir datos.

Recomendaciones

Para ayudar en el control de la información que se comparte se recomienda documentar la descripción de cada campo que contiene el archivo de acuerdo con su posición, su longitud en caso de ser de ancho fijo, su tipo de dato, si el archivo tiene o no encabezados, el conjunto de valores que maneja (por ejemplo: M o F para indicar el género), así como el carácter usado como separador.

Así como cualquier referencia relevante acerca de la obtención, procesamiento y características de la información contenida en el archivo, tales como: unidades de medida usadas, abreviaturas, relación entre los datos, por mencionar algunos.

En el ejemplo siguiente se muestran archivos de texto plano con datos ficticios de alumnos:

Características del archivo: Archivo de texto plano, la división entre registros es por salto de línea, el archivo no tiene encabezados y cada registro tiene los datos siguientes separados por comas.

Número de cuenta	Número de cuenta del alumno.	varchar(10)
CURP	CURP del alumno.	varchar(18)
Nivel de estudios	Nivel de estudios de acuerdo con el catálogo siguiente: INICIACIÓN UNIVERSITARIA, BACHILLERATO, LICENCIATURA, MAESTRÍA, DOCTORADO, ESPECIALIDAD	varchar(15)
Plantel	Clave del plantel de adscripción del alumno.	varchar(3)
Carrera	Clave de la carrera del alumno, si el alumno se encuentra inscrito en dos o más planteles y carreras, cada inscripción estará en una línea diferente del archivo.	varchar(2)

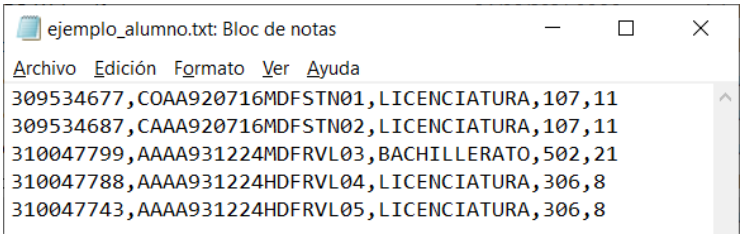


Figura 2. Ejemplo de archivo palno (txt)

Hojas de cálculo

Características

Las hojas de cálculo permiten compartir datos fácilmente, debido a que pueden ser leídas por máquinas y humanos. Es suficiente con que el usuario que solicita la información cuente con un programa de software comercial o libre para su lectura.

Sin embargo, si la entidad o dependencia universitaria que solicita los datos así lo determina, puede establecer procesos automáticos o manuales para la incorporación, lectura o transformación de los datos contenidos en los archivos.

Recomendaciones

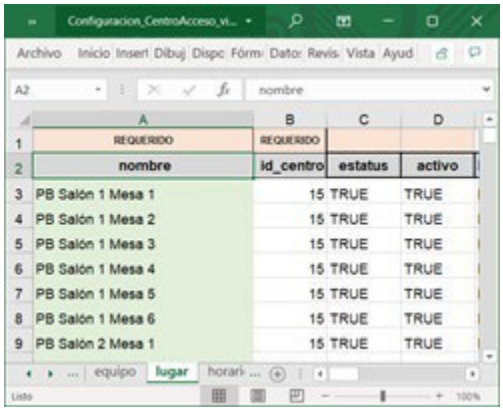
Para que se facilite el control de la información a compartir entre áreas universitarias es aconsejable documentar el contenido del archivo indicando la descripción del dato que contiene cada columna, su tipo de dato e indicar si cada columna tiene encabezados, a partir de qué renglón se presentan los datos y el conjunto de valores que se pueden encontrar. En caso de ser un libro, indicar la información de cada hoja y si existe relación entre ellas.

De igual manera, se pueden indicar datos adicionales que sean de utilidad para el entendimiento del contenido en la hoja de cálculo y su procesamiento, tales como: fórmulas utilizadas en caso de que las incluya o características de la obtención de la información, por mencionar algunas.

En el ejemplo siguiente, se muestra la descripción de un archivo de Excel que contiene los lugares de un centro de cómputo y la imagen del contenido de un archivo. El archivo tiene una primera fila para indicar si el dato es requerido y una segunda fila con los encabezados.

nombre	Nombre del lugar, con el que se podrá ubicar el lugar dentro del centro de cómputo. El orden en que se registren indicará el orden en que los lugares serán asignados.	varchar(100)
id_centro	Identificador del centro de cómputo.	Integer
estatus	Estatus del lugar. TRUE = disponible, FALSE = ocupado. Para que pueda ser usado en la operación del centro necesitaría tener asignado el valor de TRUE.	Boolean

activo	Indica si el lugar está activo o inactivo, para que el lugar pueda ser usado por el alumno o profesor durante el préstamo de equipo al inicio de la operación se debe asignar el valor de TRUE.	Boolean



	A	B	C	D
1	REQUERIDO	REQUERIDO		
2	nombre	id_centro	estatus	activo
3	PB Salón 1 Mesa 1	15	TRUE	TRUE
4	PB Salón 1 Mesa 2	15	TRUE	TRUE
5	PB Salón 1 Mesa 3	15	TRUE	TRUE
6	PB Salón 1 Mesa 4	15	TRUE	TRUE
7	PB Salón 1 Mesa 5	15	TRUE	TRUE
8	PB Salón 1 Mesa 6	15	TRUE	TRUE
9	PB Salón 2 Mesa 1	15	TRUE	TRUE

Figura 3. Ejemplo de archivo en Excel

La información contenida en el Excel la puede utilizar el receptor de la información de diferentes formas como pueden ser: usando directamente la información del archivo de Excel para reportes o gráficas generadas de forma manual en el mismo archivo o los fines que tenga establecidos, para importar en una base de datos mediante alguna herramienta o módulo de un sistema desarrollado para este fin. Por ejemplo:

Figura 4. Ejemplo de importación de archivo

Archivos con formato JSON

Características

Los archivos en formato JSON (JavaScript Object Notation) son ligeros y útiles para compartir datos, son sencillos de leer y escribir para los humanos, además de ser fáciles de generar e interpretar por las máquinas. JSON está basado en el subconjunto del estándar del lenguaje de programación ECMA-262 tercera edición - diciembre de 1999.

Este formato es el que se suele utilizar en los servicios web con API REST o Ajax. Los procesos de lectura, transformación y explotación de los datos pueden ser incorporados en sistemas ya existentes o aplicaciones nuevas debido a que este puede ser procesado por componentes

desarrollados en lenguajes como: C, C++, C#, Java, JavaScript, Perl, Python, entre otros (JSON, 2020) y ha sido adoptado por algunas bases de datos, como MongoDB. Algo que ofrece este formato es que, al ser independiente de cualquier lenguaje de programación, los servicios que comparten información por este método no necesitan hablar el mismo lenguaje, es decir, el emisor puede ser Java y el receptor Python, ya que cada uno tiene su propia librería para codificar y decodificar cadenas en este formato.

JSON está construido con dos estructuras:

- Una colección de pares nombre/valor.
- Una lista ordenada de valores (arreglo).

Recomendaciones

Para facilitar el intercambio de información es aconsejable documentar la estructura que contendrán los archivos JSON, la información relevante, la forma en que se obtiene, su procesamiento, considerando describir las colecciones de pares nombre/valor que contiene el archivo, indicando el nombre, una breve descripción del dato y el tipo de dato que tienen cada elemento que integra la colección, entre otros.

En el ejemplo siguiente se puede observar el catálogo de algunas materias de convenios:

materia_id	Identificador único de la materia de convenios.	Integer
materiaNombre	Nombre de la materia de convenios.	varchar(255)
materiaActivo	Indica si la materia del convenio se encuentra activa, acepta los valores: sí y no.	varchar(2)

materia.json

```
[
{"type":"header","version":"5.0.1","comment":"Ejemplo de archivo json"},
{"type":"database","name":"sistema_materia"},
{"type":"table","name":"materia","database":"sistema_materia","data":
[
{"materia_id":"3","materiaNombre":"DIFUSION DE LA CULTURA","materiaActivo":"si"},
{"materia_id":"6","materiaNombre":"ASIGNACION DE RECURSOS","materiaActivo":"si"},
{"materia_id":"8","materiaNombre":"INTERCAMBIO ACADEMICO","materiaActivo":"si"},
{"materia_id":"9","materiaNombre":"DESARROLLO SOCIAL","materiaActivo":"si"},
{"materia_id":"10","materiaNombre":"RETENCION EN NOMINA","materiaActivo":"si"},
{"materia_id":"11","materiaNombre":"ELECTORAL","materiaActivo":"si"},
{"materia_id":"12","materiaNombre":"INFORMATICO","materiaActivo":"si"},
{"materia_id":"13","materiaNombre":"AMBIENTAL","materiaActivo":"si"}
]
}
]
```

Figura 5. Ejemplo de la estructura en un archivo JSON

Bases de datos

Características

Los datos se pueden compartir por medio del acceso controlado a las bases de datos, tiene la ventaja de que la información se encuentra actualizada y puede consultarse desde la fuente primaria, facilitando los trámites y servicios que se realizan a partir de esta.

Recomendaciones

a) Configuración

Una parte fundamental para proteger la información que contiene una base de datos es la configuración del Sistema Manejador de Bases de datos que se utilice, por lo que se recomiendan las siguientes medidas:

- Una forma de evitar ser atacados es deshabilitar todos los servicios, procedimientos, cuentas de invitados, bases de datos de ejemplo, entre otros.
- Siempre que sea posible, es aconsejable que la base de datos no tenga acceso directamente desde Internet, para evitar que la información quede expuesta a posibles atacantes remotos.

b) Acceso

Cuando se comparte la información permitiendo el acceso a bases de datos, es importante considerar el entorno y cuestiones de seguridad a revisar. Se sugiere realizar un análisis de la información a compartir y restringir el ingreso otorgando sólo los permisos indispensables para satisfacer la solicitud de datos aprobada.

A través de la creación de usuarios y grupos con permisos específicos acorde al tipo de información que se desee acceder, es posible restringir el acceso a información sensible o confidencial.

Otra forma de hacerlo es mediante el uso de vistas, con las cuales se puede ocultar la estructura de las tablas a ciertos usuarios, en donde este no sabrá que existen atributos que se han omitido al definir la vista. Otra alternativa es ejecutar procedimientos almacenados que sólo estén autorizados a realizar consultas a la información.

Para una mayor protección de las bases de datos, se pueden controlar los accesos a nivel de las direcciones IPs para exclusivamente aquellos equipos que se requieran.

Adicionalmente, una buena práctica siempre que sea posible, es restringir el acceso fuera del horario laboral o habitual.

c) Uso de la información

Para pruebas de sistemas, una buena práctica en el uso de las bases de datos es el enmascaramiento o anonimato de las mismas, en donde se conserva la estructura, pero se modifican los valores de los datos sensibles (mezclándolos entre sí, cifrándolos, combinando los caracteres o sustituyendo palabras) para que permanezcan protegidos.

La encriptación de datos sensibles puede utilizarse a nivel de las bases de datos, como es el caso de las contraseñas, pero debe realizarse primero un análisis del impacto en el

rendimiento, de la seguridad requerida al tipo de información y su valor, así como el posible cumplimiento normativo que le pueda aplicar. Es necesario asegurarse de que se estén utilizando algoritmos robustos y vigentes para cifrarlos.

d) Auditoría y monitoreo

Para revisar accesos y modificación de datos no autorizados en las bases de datos es importante auditar y registrar las acciones y movimientos que se realizan sobre ellos en la base de datos, lo cual permitirá conocer quién, qué, cuándo y cómo se ha manipulado la información.

e) Documentación

Contar con un diccionario de datos actualizado, claro y detallado es una buena práctica para lograr el entendimiento entre el solicitante de los datos y el responsable (dueño) que tiene bajo su resguardo la base de datos, así mismo documentar los accesos otorgados para facilitar las labores de revisión y seguridad de la información.

Sistemas de información y aplicaciones

Los sistemas informáticos deben atender el manejo de la información acorde a su clasificación y a las buenas prácticas.

Recomendaciones

Se sugiere proteger la información implicada en transacciones en línea para prevenir la transmisión incompleta, la omisión de envío, la alteración no permitida del mensaje, la divulgación no autorizada y la duplicación o repetición no establecida, además de considerar la normatividad aplicable al tipo de información.

Así, por ejemplo, en el caso de portales o sistemas que manejan información confidencial o sensible o que den un servicio crítico, se recomienda que las conexiones a ellos sean cifradas y las páginas seguras con protocolos HTTPS (Hypertext Transfer Protocol Secure) y TLS 1.2 o superior (Transport Layer Security), que ayudan a ocultar y proteger los datos enviados y recibidos en los navegadores.

Otras formas de protección son restringir los tiempos de conexión o terminar las sesiones inactivas después de un período de inactividad preestablecido, con lo cual se puede reducir la ventana de oportunidades para el acceso no autorizado.

Recomendaciones de seguridad para la compartición de información

a) Controles de acceso

- Restringir para que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
- Limitar el acceso físico y lógico a los servidores de gestión documental o repositorios de información confidencial o sensible.

- Utilizar doble factor de autenticación para sistemas que manejan información confidencial o sensible.
- Ejecutar un procedimiento de verificación periódico de los derechos de acceso de los usuarios.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados a los sistemas de información, bases de datos y carpetas compartidas, controlando los derechos de acceso de los usuarios (por ejemplo, de lectura, escritura, borrado y ejecución).
- Utilizar contraseñas seguras para acceder o realizar la conexión a los sistemas de información o las bases de datos. Para la generación de las contraseñas considerar al menos lo siguiente:
  - No podrá ser asociada con facilidad a cualquier información relacionada con el usuario de la cuenta.
  - Tener una longitud mínima de ocho (8) caracteres, combinando letras mayúsculas y minúsculas, signos de puntuación (- * ? ! @ # $ / () {} = . , ; :) y números. No utilizar acentos, ni caracteres acentuados. Lo más recomendable es que tenga entre 8 y 12 caracteres.
  - No utilizar la misma contraseña para todas las cuentas o usuarios.
- Almacenar archivos de contraseñas en lugares diferentes de los datos del sistema de aplicaciones, en formatos protegidos.
- Aplicar políticas de bloqueo de contraseñas, de modo que después de determinado número de intentos fallidos (se recomienda hasta 3 intentos), el acceso mediante contraseña quede bloqueado o se utilicen métodos de retardo de solicitud de contraseña, es decir, no se pueda acceder hasta después de cierto tiempo.
- Cambiar la información de autenticación siempre que existan indicios de su posible compromiso.

b) Comunicación y transmisión

- Llevar a cabo las transacciones de datos sensibles sólo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío y de recepción, así como de no repudio del origen.
- Restringir las direcciones IP desde donde se van a originar las conexiones.
- Para acceder a información sensible o confidencial desde otros lugares en el Internet o redes no seguras, se puede hacer uso de una conexión segura a través de una Red Privada Virtual (VPN por sus siglas en inglés) para que la información se transmita cifrada a 128 bits como mínimo.
- Cuando se trate de intercambios periódicos de información se deberá privilegiar la "transmisión de datos" a través de canales seguros, utilizando mecanismos como: protocolos IPsec, SSL/TLS, VPN, túneles punto a punto, llaves públicas o privadas, entre otros.
- Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos) para autorizar el acceso y controlar los flujos de información desde y hacia las redes.
- Establecer una cadena de custodia mientras la información se encuentra en tránsito.
- Para información no crítica, se aconseja verificar por lo menos la autenticidad del otro extremo de la comunicación, es decir corroborar que quien hizo la solicitud sea quien dice ser, antes de proceder al intercambio de información. Además de realizar verificaciones sobre su integridad y confiabilidad al ser transmitida.

- Usar controles criptográficos para la protección de la confidencialidad, integridad y autenticidad de la información sensible o confidencial que sea almacenada o transmitida. Por ejemplo, contraseñas o datos bancarios, de modo que sea ininteligible para todos excepto para las entidades o dependencias autorizadas.
- Emplear funciones de cifrado y descifrado, gracias a que proporcionan una capa adicional de seguridad, siendo la criptografía simétrica más vulnerable que la asimétrica por el hecho de usar una única llave. Por otro lado, la encriptación simétrica es más rápida que la asimétrica y esto la favorece ya que el tiempo de descifrado llega a ser importante en algunos contextos.
- En caso de que se comprometan las contraseñas de las cuentas para intercambio es aconsejable bloquearlas y cambiarlas, realizando un análisis de la causa que originó la brecha de seguridad.
- Para corroborar la integridad de la información sensible o crítica que se transmita se pueden utilizar funciones Hash de 256 bits como mínimo.

c) Auditoría y monitoreo

- Contar con registros de auditoría asociados a las conexiones que accedieron a la información sensible o confidencial, almacenando los siguientes datos:
  - Dirección IP origen de las conexiones.
  - Hora inicio y fin de la conexión.
  - Usuario.
  - Comandos ejecutados.
  - Archivos accedidos.
- Realizar pruebas de seguridad regulares, para identificar, monitorear y reportar las vulnerabilidades y los incidentes detectados.
- Establecer controles para detectar y resolver accesos no autorizados a la información, aplicaciones e infraestructura. En su caso, tomar las medidas correspondientes y de ser afectados los datos personales considerar las acciones establecidas en la normatividad.

Bibliografía y referencias electrónicas

- Cámara de Diputados (2017). **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lgpdppso.htm
- Cámara de Diputados (2018). **Código de Comercio**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/ccom.htm
- Cámara de Diputados (2018). **Ley General de Archivos**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lga.htm
- Cámara de Diputados (2020). **Ley Federal del Derecho de Autor**. Recuperado: el 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lfda.htm
- Cámara de Diputados (2020). **Ley Federal de Protección a la Propiedad Industrial**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lfppi.htm
- Cámara de Diputados (2021). **Constitución Política Mexicana**. Recuperado: 28 de

junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm

- Cámara de Diputados (2021). **Código Fiscal de la Federación**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/cff.htm
- Cámara de Diputados (2021). **Código Penal Federal**. Recuperado: 28 de junio de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/cpf.htm
- Cámara de Diputados (2021). **Ley General de los Derechos de Niñas, Niños y Adolescentes**. Recuperado: 9 de septiembre de 2021. URL: http://www.diputados.gob.mx/LeyesBiblio/ref/lgdnna.htm
- Diario Oficial de la Federación (2016). **Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos**. Recuperado: 28 de junio de 2021. URL: http://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html
- Diario Oficial de la Federación (2017). **Lineamientos Generales de Protección de Datos Personales para el Sector Público**. Recuperado: 05 de abril de 2022. URL: http://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018
- INAI (2018). **Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales**. Recuperado: 05 de abril de 2022. URL: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/ComputoEnLaNube.pdf
- INAI (2020). **Acuerdo mediante el cual se aprueba la Adición del Título Décimo a los Lineamientos Generales de protección de datos personales para el sector público**. Recuperado: 05 de abril de 2022. URL: https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf
- Instituto Nacional de Ciberseguridad (2016). **Guía de almacenamiento seguro de la información**. Recuperado: 05 de abril de 2022. URL: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad.pdf
- ISO (2013). ISO-IEC_27002-2013 Code of practice for IS management.
- IT Governance Institute (2007), **COBIT 4.1**.
- JSON (2020). **Introducción a JSON**. Recuperado: 24 de noviembre de 2020. URL: https://www.json.org/json-en.html
- UNAM (2016). **Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México**. Recuperado: 9 de septiembre de 2021. URL: http://www.transparencia.unam.mx/files/documentos/reglamento_transparencia2016.pdf
- UNAM (2017). **Lineamientos y recomendaciones para la Administración de Bases de Datos**. Recuperado: 28 de junio de 2021. URL: https://www.red-tic.unam.mx/node/74

- UNAM (2018). **Lineamientos Generales para la Organización, Administración y Conservación de los Archivos de la Universidad Nacional Autónoma de México**. Recuperado: 28 de junio de 2021. URL: https://www.red-tic.unam.mx/recursos/LineamientosArchivosUNAM.pdf
- UNAM (2020). **Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad**. Recuperado: 28 de junio de 2021. URL: https://www.gaceta.unam.mx/wp-content/uploads/2020/01/200130-convocatorias.pdf

Créditos

Rector
Dr. Enrique Luis Graue Wiechers

Secretaria de Desarrollo Institucional
Dra. Patricia Dolores Dávila Aranda

Director General de Cómputo y de Tecnologías de Información y Comunicación
Dr. Héctor Benítez Pérez

Coordinación
MATIE. Alberto González Guízar
Mtra. Irene Sánchez García

Elaboración
José Othoniel Chamú Arias - DGTIC
Susana Laura Corona Correa - DGTIC
José Luis Chávez Sánchez- DGTIC
Alberto González Guízar- DGTIC

Revisión
Fernando Israel González Trejo - FES Acatlán
Miguel Ángel Jiménez Bernal - DGBSDI
Leticia Martínez Calixto - DGTIC
Ana Pérez Arteaga - IIMAS
Hugo Alonso Reyes Herrera – DGTIC

Autorización de publicación en sitio de la RedTIC
Dra. Marcela Peñaloza Báez